

STATE OF COLORADO
Department of State

1700 Broadway, Suite 270
Denver, CO 80290



Mike Coffman
Secretary of State

Holly Lowder
Director, Elections

DRAFT – 3/13/2008

THIS IS A DRAFT FOR PUBLIC COMMENT.

PLEASE SUBMIT WRITTEN COMMENTS BY 5 P.M. ON MARCH 18, 2008 TO STEPHANIE CEGIELSKI AT
STEPHANIE.CEGIELSKI@SOS.STATE.CO.US

Conditions for Use – SEQUOIA - AMENDED 3/13/08

The Testing Board would also recommend the following conditions for use of the voting system. These conditions are required to be in place should the Secretary approve for certification any or all of the items indicated in the **COMPONENTS** section. **THE TESTING BOARD HAS MODIFIED THE CONDITIONS BASED ON INFORMATION PROVIDED THROUGH PUBLIC HEARING UNDER LEGISLATIVE UPDATES TO CONSIDER ADDITIONAL PROCEDURES. ANY DEVIATION FROM THE CONDITIONS PROVIDES SIGNIFICANT WEAKNESS IN THE SECURITY, AUDITABILITY, INTEGRITY AND AVAILABILITY OF THE VOTING SYSTEM.** ~~Being that many conditions address the security, auditability and availability of the system component, the testing board would firmly reject any option which removes, replaces or diminishes the conditional requirement and still allow the system to be used and recommended for certification. Any "Y" value in the recommendation table would change to a "N" value with any change to the conditions.~~

Global Conditions (applies to all components):

- 1) Modem and other telecommunication devices may not be used on any subsystem component - system provider was unable to meet or provide prerequisite FIPS 140/180 certifications.
- 2) Provisional ballots must be processed separately from non-conditional ballots - system subcomponents are unable to functionally differentiate and correctly process to Colorado specific requirements.
- 3) Coordination of Escrow Setup - Upon Certification, voting system manufacturer must coordinate the Escrow of the TRUSTED BUILD software with SOS escrow, or third party escrow service as required by Rule 11 prior to use in Colorado.
- 4) Abstract Report Generation - abstracts used for State reporting must come from WinEDS Software, or other external solution, rather than from the specific device.
- 5) Trusted Build Verification (all software and firmware components)
 - a) The system components do not allow for proper verification of trusted build software. Any breach of custody and/or other security incidents will require the rebuild of the component with the state trusted build software. This requirement applies to all voting devices, firmware and software

components of the system.

b) Counties shall ensure that hardware, software and firmware purchased for use of the system matches the specifications of VSTL/EAC and/or State Certified and trusted versions, not to the version presented in the vendor documentation.

6) Counties using the voting system shall testify through their security plan submission that the voting system is used only on a closed network.

Software Conditions (WinEDS 3.1.074):

1) System/Database/Network Security Hardening.

a) Because the voting system operates in a non-restricted system configuration containing open file system access to locate, copy, open and overwrite without detection, election vote content database files outside of election management system application by third-party tools, counties will be required to modify their physical environmental conditions, or work with current Sequoia documentation (not currently tested) and request variance from the Secretary of State to use Sequoia hardening documentation in lieu of environmental changes. COUNTIES SHALL SUBMIT THEIR PLAN FOR APPROVAL TO THE SECRETARY OF STATE'S OFFICE TO BE INCLUDED IN THE COUNTY SECURITY PLAN ON OVERCOMING THESE CONDITIONS THROUGH COUNTY ENVIRONMENTAL AND/OR PROCEDURAL CHANGES WHERE POSSIBLE. ~~If approved, counties shall submit plans for approval to the Secretary of State's office on overcoming these conditions through one of the two stated processes.~~

~~b) b)~~ In addition to physical environmental changes, counties shall MAINTAIN THE INTEGRITY OF THE MASTER WINEDS DATABASES WITH ONE OF THE FOLLOWING TWO METHODS:

OPTION #1 - ~~e~~C Create a second (or backup) copy of the WinEDS database that is created immediately after the point of memory card downloads. The backup copy shall be stored on closed CD Media and documented as matching the master database. This process shall be observed by two election staff members. Chain of custody documents shall be generated for the media, and the media shall be sealed with at least two tamper evident seals and stored in a sealed or lockable transfer case that is stored in a limited access area. ~~AFTER the close of polls~~ ON ELECTION DAY, the designated election official shall load the sealed copy of the database onto the server and proceed with uploading memory cards after documenting the loading of the backup master database onto the system. After loading the sealed database copy, the county shall re-secure the database with seals (updating necessary logs) in the limited access location; OR

OPTION #2 - CREATE A SECOND (OR BACKUP) COPY OF THE WINEDS DATABASE THAT IS CREATED IMMEDIATELY AFTER THE POINT OF DOWNLOADING ALL MEMORY CARDS. THE COPY OF THE DATABASE WILL BE ESCROWED WITH THE COLORADO SECRETARY OF STATE'S OFFICE ALONG WITH THE "PROFILE" DATABASE. AFTER EACH OF THE EVENTS DESCRIBED BELOW, THE COUNTY SHALL PROVIDE BOTH AN UPDATED COPY OF THE DATABASE TO THE SECRETARY OF STATE'S OFFICE, AN UPDATED SQL AND WINEDS AUDIT LOG, AND THE FORENSIC ANALYSIS OF THE SQL DATABASES (BOTH PROFILE AND ELECTION DATABASES) PERFORMED BY A COMMERCIALLY AVAILABLE FORENSICS TOOL, IDENTIFYING CHANGES TO DATABASE PROPERTIES SINCE THE LAST REPORT. EVENTS TRIGGERING A REPORT UPDATE TO THE SECRETARY OF STATE INCLUDE: ANY DOWNLOAD OF MEMORY CARDS, ANY UPLOAD

OF MEMORY CARDS, COMPLETION OF L&A TESTING, AND COMPLETION OF POST-ELECTION AUDIT. REPORTS ARE TO BE SUBMITTED TO THE SECRETARY OF STATE'S OFFICE WITHIN 24 HOURS OF THE EVENT.

COUNTIES SHALL INDICATE IN THEIR SECURITY PLAN WHICH OPTION THEY WILL BE EXECUTING TO MEET THE SECURITY REQUIREMENTS.

c) Additionally, to overcome deficiencies in security and auditing of the system, the county will be required to perform increased Election Night and Post Election Audits for this system. All post-election audit data shall process a hand count of paper ballots which shall match the totals report from the specific device, as well as the totals for the WinEDS database. Counties shall prepare for this event with one of two methods:

Option #1 – Prepare for the upload of memory cartridges as normal. Print necessary zero report. Upon uploading each individual memory card, print a summary report showing the change in totals from the upload of the memory card. Label the report to match the name/number of the memory card uploaded. Continue to upload memory cards and print totals reports to match. When auditing a specific device, use the difference between the report totals for the memory card selected for the audit and the totals from the immediately preceding memory card report to calculate vote totals generated by the WinEDS software.

When memory cards are delivered to the county for upload, the machine generated report shall be delivered for inspection as well. ~~On election night~~ **DURING THE POST-ELECTION AUDIT**, when the summary report indicated above is created, the difference totals (delta report) are ~~immediately~~ compared to the totals from the report generated by the device at the polling place. If the reports match, the public is ensured that the totals from the polling place match the totals from the county server. If the totals are different, the county is to report the situation (~~on election night~~) to the Secretary of State's **OFFICE** for audit, security and remedy procedures.

During the post election audit process, the totals of the paper record for the specific device are to be hand counted and verified against the electronic record for the device. The canvass board shall report the verification of three totals to match – the paper record of the device, the totals of the electronic vote on the device, and the totals in the central count server; OR

Option #2 – Prepare for the upload of memory cartridges by creating one master default database (containing all memory cards/cartridges). Create individual databases to contain values (upload data) for each separate memory card (or in some instances by batch of ballots – see condition #4b under Central Count devices. Upload memory card/cartridges into master database, and into the specific database created for that memory card (two separate uploads). This process **CAN TAKE PLACE ANY TIME AFTER THE CLOSE OF POLLS INCLUDING THROUGH THE CANVASS PERIOD.** ~~must happen on Election Night and~~ with observation by at least two people. Election summary reports shall be printed from each individual database and manually added together. The totals from the individual databases must match the master database before proceeding. Upon verification that the master and individual databases match, the county can then use the individual reports to conduct a hand count of the paper ballot (or paper record) generated by the device to show that the WinEDS totals match. The verification of the separate upload databases verify that the database totals match the field totals on each memory card device, as was designed after the point of Logic

and Accuracy testing took place.

2) Audit Trail Information.

a) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the WinEDS software for processing by other methods.

b) Operators of the system shall also be required to maintain logs indicating use of the report printing functions of the software, and detailed information to changes of the system including hardware changes which shall include: insert removable media, remove removable media, modify system hardware drivers, modify system physical hardware, and any other system property changes made by either judges or other trusted staff. Logs shall be maintained physically in a file outside or separate from the database, which is NOT accessible for review and/or modification by user/operator accounts on the system, but that is readily accessible to election officials or other interested party.

3) Trusted Build Protection.

Applies to WinEDS software and custom components of SQL server as applicable. Refer to Global Condition #5a for ensuring integrity of trusted build.

4) Performance Deficiencies.

Due to failures in performance, counties shall allow extra time for downloads and uploads of memory card devices. This may impact programming, testing and use of the system on election night. Counties shall ensure trusted staff is properly trained on this issue and accommodating the allowable time required for programming memory devices.

5) Provisional Ballots.

The software is not capable of processing provisional ballots internally to accept federal and state only questions. A procedure outside of the voting system will be required. Additionally, the abstracts and reports created by the software do not meet the requirements of rule 41.6.3(g) and users of the system will be required to generate an abstract outside of the voting system.

6) Election Database Creation and Testing.

The system relies heavily on an external program called BPS which typically is used for importing the ballot setup process into WinEDS. Since this program is to be considered non-trusted and is not third party as it is made by the voting system manufacturer, the program shall only be able to receive data from WinEDS. WinEDS shall not be used to import data from BPS, UNLESS THE DATA IS IN A STATIC IMPORT FILE FORMAT SUCH AS A FLAT FILE, CSV, TXT, OR SIMILAR WHICH CAN BE IMPORTED WITHOUT THE USE OF VENDOR PROPRIETARY SOFTWARE. Additional testing will therefore be required by counties for both electronic and paper ballots to ensure all voting positions are working as designed prior to each election. This shall include ordering a complete set of at least ~~5~~4 ballots of each style that contain the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly.

Precinct Count Scanner Conditions (Insight/Insight Plus):

1) Intrusion Seals for Protection of Trusted Build Firmware.

Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

2) External ~~Battery Backup~~ **POWER SUPPLY (UPS) Devices Required. REQUIRED**

THE DEVICE CONTAINED INTERNAL POWER TO RUN FOR THREE HOURS, HOWEVER UNDER THE INTERNAL BATTERY INCLUDED WITH THE SYSTEM, THE DEVICE DID NOT COUNT VOTES CORRECTLY. USING AN EXTERNAL POWER SOURCE SUCH AS A UPS UNIT PROVIDING BATTERY POWER ALLOWS THE DEVICE TO MEET THE POWER REQUIREMENT AND COUNT CORRECTLY. ~~Insufficient internal power reserves to sustain minimum 3-hour continuous operation.~~ Counties shall purchase and use an external power supply that meets or exceeds the vendor's recommendation for ~~the~~ **EACH** component.

3) Device Security Accessibility.

- a) Device level administrative functions requiring access involving the use of keys, memory cards, and passwords must be restricted to **NO MORE THAN TWO (2)** ~~single~~ person entry with detailed logs.
- b) County use of voting system will require use of WinEDS Software to modify the "administrator" password on the voting device.

4) Ballot/Race Conditions Simulation.

Additional County testing shall be required to accommodate ballots with conditions from each election. This shall include ordering a complete set of at least ~~5~~ **4** ballots of each style that contain the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly.

5) Audit Trail Information:

- a) Operators of the system shall also be required to maintain logs indicating use of the administrator functions of the device by either judges or other trusted staff.
- b) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the WinEDS software for processing by other methods.
- c) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include the verification of the hand count of paper ballots to match the totals generated from the WinEDS software as indicated in Software condition #1c.

6) Voting Secrecy.

Insufficient privacy of ballot was detected using secrecy sleeve. Election administrators must ensure system secrecy sleeve (from Sequoia) is used for ballots up to 14". For longer ballots, the counties shall create a secrecy sleeve to accommodate the deficiency and submit design form to Secretary of State for approval.

Central Count Scanner Conditions (400-C):

1) Intrusion Seals for Protection of Trusted Build Firmware.

Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated. Refer to Global Condition #5a for ensuring integrity of trusted build.

2) System/Database/Network Security Hardening.

Because the voting system operates in a non-restricted system configuration containing open file system access to locate, copy, open and overwrite without detection, election vote content database files outside of election management system application by third-party tools, counties will be required to modify their physical environmental conditions, or work with current Sequoia documentation (not currently tested) and request variance from the Secretary of State to use Sequoia hardening documentation in lieu of environmental changes. If approved, counties shall submit plans for approval to the Secretary of State's office on overcoming these conditions through one of the two stated processes.

3) External ~~Battery backup~~ POWER SUPPLY (UPS) Devices Required.

Insufficient internal power reserves to sustain minimum 3 hour continuous operation. Counties shall purchase and use an external power supply that meets or exceeds the vendor's recommendation for the component. ACCEPTABLE POWER SUPPLY SOURCES INCLUDE GENERATORS AND OTHER FACILITY BASED SOLUTIONS.

4) Audit Trail Information:

a) Judges shall be required to include device serial number on all reports regarding use of the device. Additionally, the county shall include the device serial number on applicable reports from the device.

b) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include a hand count of at least THE FOLLOWING AMOUNT OF BALLOTS COUNTED ON THE DEVICE FOR THE SPECIFIC RACES SELECTED IN THE POST ELECTION AUDIT:

<u>TOTAL # OF BALLOTS COUNTED ON DEVICE:</u>	<u>TOTAL # OF BALLOTS TO AUDIT:</u>	<u># OF ERRORS REQUIRING ESCALATION:</u>
<u>150,000 TO 500,000</u>	<u>1,250</u>	<u>6</u>
<u>35,001 TO 150,000</u>	<u>800</u>	<u>4</u>
<u>10,001 TO 35,000</u>	<u>500</u>	<u>3</u>
<u>3,201 TO 10,000</u>	<u>315</u>	<u>2</u>
<u>1,201 TO 3,200</u>	<u>200</u>	<u>2</u>
<u>501 TO 1,200</u>	<u>125</u>	<u>2</u>
<u>281 TO 500</u>	<u>80</u>	<u>1</u>
<u>151 TO 280</u>	<u>50</u>	<u>1</u>
<u>91 TO 150</u>	<u>32</u>	<u>1</u>
<u>51 TO 90</u>	<u>20</u>	<u>1</u>
<u>26 TO 50</u>	<u>13</u>	<u>1</u>
<u>16 TO 25</u>	<u>8</u>	<u>1</u>
<u>9 TO 15</u>	<u>5</u>	<u>1</u>
<u>1 TO 8</u>	<u>3 OR 100% IF LESS THAN 3</u>	<u>1</u>

ERRORS DETECTED DURING THE MANUAL AUDIT PROCESS SHALL BE RESOLVED ACCORDING TO C.R.S. 1-7-514, AND SECRETARY OF STATE RULE 11. ERRORS DISCOVERED EXCEEDING THE ERROR RATE IDENTIFIED IN THE TABLE ABOVE SHALL REQUIRE ESCALATION MEASURES INCLUDING INCREASED AUDITS AS PRESCRIBED BY THE SECRETARY OF STATE'S OFFICE. COUNTY OFFICIALS SHALL CONTACT THE SECRETARY OF STATE'S OFFICE AS SOON AS POSSIBLE IF AN AUDIT DETECTS ERRORS ABOVE THE ESCALATION THRESHOLD.

~~the following amounts of ballots:~~

~~Considering the closest race in the election, if the difference between the top two candidates for the race is:~~

~~10% or greater, then hand count 60 ballots for every 10,000 cast;
9.00%—9.99%, then hand count 65 ballots for every 10,000 cast;
8.00%—8.99%, then hand count 70 ballots for every 10,000 cast;
7.00%—7.99%, then hand count 80 ballots for every 10,000 cast;
6.00%—6.99%, then hand count 95 ballots for every 10,000 cast;
5.00%—5.99%, then hand count 115 ballots for every 10,000 cast;
4.00%—4.99%, then hand count 140 ballots for every 10,000 cast;
3.00%—3.99%, then hand count 185 ballots for every 10,000 cast;
2.00%—2.99%, then hand count 275 ballots for every 10,000 cast;
1.00%—1.99%, then hand count 550 ballots for every 10,000 cast;
0.01%—0.99%, then hand count 1200 ballots for every 10,000 cast.~~

The verification of the hand count of paper ballots shall match the totals generated from the WinEDS software as indicated in Software condition #1c. Counties shall load only the master database from the secured storage location for processing the post election audit ballots as indicated in Software Condition #1b. Counties shall prepare database and batches of ballots prior to scanning into system (for election results) to accurately generate reports in batch sizes as necessary for the audit. ~~If the county or system is not capable of accommodating the requirement of batch size after the outcome of the election is revealed, the highest percentage of ballots shall be used for the audit process.~~

c) Additional County testing shall be required to accommodate ballots with conditions listed. This shall include ordering a complete set of at least ~~5~~ 4 ballots of each style that contain the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly.

5) Device Security Accessibility.

Device level administrative functions requiring access involving the use of keys, memory cards, and passwords must be restricted to no more than two (2) ~~single~~-person entry with detailed logs.

DRE Conditions (Edge2):

1) External ~~Battery Backup~~ POWER SUPPLY ~~(UPS) Devices~~ Required.

Insufficient internal power reserves to sustain minimum 3 hour continuous operation. Counties shall

purchase and use an external power supply that meets or exceeds the vendor's recommendation for the component TO ACCOMMODATE A 90 MINUTE SHORT COMING EXPERIENCED BY THE TESTING BOARD DURING TESTING OF THE DEVICE.

2) Intrusion Seals for Protection of Trusted Build Firmware.

Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

3) Ballot/Race Conditions Simulation.

Additional County testing shall be required to accommodate ballots with conditions listed. This shall include ordering a complete set of at least ~~5~~ 4 ballots of each style that contain the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly. All ballots in this detail shall be "marked" using the DRE device as applicable for similar testing.

4) V-VPAT Paper Record Shall be Handled per Rule 11.6.

- a) Prescribed paper record is of the thermal type and requires special storage conditions to avoid legibility degradation. Counties shall follow the requirements for handling according to Secretary of State Rule 11 and 43.
- b) Election judges are required to perform the "Printer Test" in between paper changes and verify with one additional judge that the paper has been loaded correctly and is printing according to design which ensures that all machines will have paper records for each vote cast.

5) V-VPAT Security.

The V-VPAT device provides no assurance that it cannot accommodate other devices, and/or the device is a standard communication port. This connection between the V-VPAT printer and the DRE unit shall be secured with tamper evident seals with proper chain of custody documentation to prevent and detect tampering.

6) Accessible Distances.

Operators of the system shall be required to provide an accessible solution by operating the device on a separate table. The manufacturer's stand does not meet accessible reaches as outlined in 1-5-704. Counties shall be educated on these measurements and ensuring that the table top solution complies with the requirements. THIS CONDITION COULD ALSO BE ACHIEVED WITH THE USE OF A REACH STICK THAT IS AT LEAST 4" IN LENGTH. SHOULD THE COUNTIES USE THE DRE IN THE STAND WITH A REACH STICK, THE COUNTY SHALL ENSURE THAT A SIDE APPROACH BY A WHEELCHAIR IS POSSIBLE DUE TO THE DEFICIENCIES IN THE KNEE CLEARANCE (DEPTH AND WIDTH) OF THE STAND.

7) Accessible Operation.

Due to the inability for the voter to pause and resume the audio text, election judges shall provide instructions specific to this fact to the voters and operations for repeating the text if text was missed, which shall include details on navigating forward and backwards through the system prompts.

8) Audit Trail Information:

- a) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the WinEDS software for processing

by other methods.

b) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include the verification of the hand count of paper records to match the totals generated from the WinEDS software as indicated in Software Condition #1c.

9) Confusing Instructions to Voters.

Due to the complicated messaging provided to voters during the V-VPAT review process, the use of the device shall require election administrators to change the wording of the review screen to properly indicate to voters that a review of the ballot is taking place.

10) Device Security Accessibility.

a) The "override.ini" file ~~must not be used with the voting system. The file~~ is not a VSTL-~~approved~~ **CERTIFIED** file, and poses **THE** potential for **A** security threat (denial of service in particular). **DUE TO THIS FACT, THE STATE WILL REQUIRE THE CREATION OF A STATE COPY OF THE FILE TO ENSURE** ~~ensuring~~ **CHANGE CONTROL AND ASSOCIATED HASH VALUES ARE PASSED TO THE COUNTIES THROUGH THE DISTRIBUTION OF THE TRUSTED BUILD. SHOULD A COUNTY REQUEST A CHANGE TO THE STATE CERTIFIED COPY OF THE FILE, THE CHANGE WILL BE MADE AND THE STATE WILL RECORD NEW HASH VALUES FOR THE FILE WHICH WILL THEN BE DEPLOYED IN A SIMILAR FASHION AS THE TRUSTED BUILD TO THE COUNTIES.**

b) Devices deployed in Colorado shall require a "lockable" activate button. ~~The button shall be protected with a tamper evident seal.~~ -Voter activation by use of the activate button shall not be used in the voting environment.

c) Device level administrative functions requiring access involving the use of keys, memory cards, and passwords must be restricted to **NO MORE THAN TWO (2)** ~~single~~-person entry with detailed logs.

DRE Conditions (Edge2plus):

~~1) External Battery Backup (UPS) Devices Required.~~

~~Insufficient internal power reserves to sustain minimum 3 hour continuous operation. Counties shall purchase and use an external power supply that meets or exceeds the vendor's recommendation for the component.~~

~~21)~~ Intrusion Seals for Protection of Trusted Build Firmware.

Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

~~32)~~ Ballot/Race Conditions Simulation.

Additional County testing shall be required to accommodate ballots with conditions listed. This shall include ordering a complete set of at least ~~5~~ **4** ballots of each style that contain the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly. All ballots in this detail shall be "marked" using the DRE device as applicable for similar testing.

43) V-VPAT Paper Record Shall be Handled per Rule 11.6.

- a) Prescribed paper record is of the thermal type and requires special storage conditions to avoid legibility degradation. Counties shall follow the requirements for handling according to Secretary of State Rule 11 and 43.
- b) Election judges are required to perform the “Printer Test” in between paper changes and verify with one additional judge that the paper has been loaded correctly and is printing according to design which ensures that all machines will have paper records for each vote cast.

54) V-VPAT Security.

The V-VPAT device provides no assurance that it cannot accommodate other devices, and/or the device is a standard communication port. This connection between the V-VPAT printer and the DRE unit shall be secured with tamper evident seals with proper chain of custody documentation to prevent and detect tampering.

65) Accessible Distances.

Operators of the system shall be required to provide an accessible solution by operating the device on a separate table. The manufacturer’s stand does not meet accessible reaches as outlined in 1-5-704. Counties shall be educated on these measurements and ensuring that the table top solution complies with the requirements. **THIS CONDITION COULD ALSO BE ACHIEVED WITH THE USE OF A REACH STICK THAT IS AT LEAST 4” IN LENGTH. SHOULD THE COUNTIES USE THE DRE IN THE STAND WITH A REACH STICK, THE COUNTY SHALL ENSURE THAT A SIDE APPROACH BY A WHEELCHAIR IS POSSIBLE DUE TO THE DEFICIENCIES IN THE KNEE CLEARANCE (DEPTH AND WIDTH) OF THE STAND.**

76) Accessible Operation.

Due to the inability for the voter to pause and resume the audio text, election judges shall provide instructions specific to this fact to the voters and operations for repeating the text if text was missed, which shall include details on navigating forward and backwards through the system prompts.

87) Audit Trail Information:

- a) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the WinEDS software for processing by other methods.
- b) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include the verification of the hand count of paper records to match the totals generated from the WinEDS software as indicated in Software Condition #1c.

98) Confusing Instructions to Voters.

Due to the complicated messaging provided to voters during the V-VPAT review process, the use of the device shall require election administrators to change the wording of the review screen to properly indicate to voters that a review of the ballot is taking place.

109) Device Security Accessibility.

A) THE “OVERRIDE.INI” FILE IS NOT A VSTL-CERTIFIED FILE, AND POSES POTENTIAL FOR SECURITY THREAT (DENIAL OF SERVICE IN PARTICULAR). DUE TO THIS FACT, THE STATE WILL REQUIRE A STATE COPY OF THE FILE ENSURING CHANGE CONTROL IS PASSED TO THE COUNTIES THROUGH THE DISTRIBUTION OF THE TRUSTED BUILD. SHOULD A COUNTY REQUEST A CHANGE TO THE STATE CERTIFIED COPY OF THE FILE, THE CHANGE WILL BE MADE AND THE STATE WILL

RECORD NEW HASH VALUES FOR THE FILE WHICH WILL THEN BE DEPLOYED IN A SIMILAR FASHION AS THE TRUSTED BUILD TO THE COUNTIES. ~~a) The “override.ini” file must not be used since it is not a VSTL approved file, and since editing the contents of this file can cause the Edge2plus to be inoperable.~~

b) Devices deployed in Colorado shall require a “lockable” activate button. The voting system vendor must provide schematics and assembly drawings of the button prior to installation and use, which must be approved by the Secretary of State prior to deployment. ~~The button shall be protected with a tamper evident seal at all times.~~ Voter activation by use of the activate button shall not be used in the voting environment.

c) Device level administrative functions requiring access involving the use of keys, memory cards, and passwords must be restricted to NO MORE THAN TWO (2) ~~single~~ person entry with detailed logs.

Insight Memory Pack Receiver Conditions (2.1.5):

1) Intrusion Seals for Protection of Trusted Build Firmware.

Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on memory cartridge & memory pack reader/burner and will require additional seals for protection against entry points as indicated by the Secretary of State. Requirements apply to physical MPR and all data cartridges used by the county. Refer to Global Condition #5a for ensuring integrity of trusted build.

Card Activator Conditions (Version 5.0.31):

1) Intrusion Seals for Protection of Trusted Build Firmware

DEVICE HAS NO PROVISION OF TRUSTED BUILD VERIFICATION ONCE INSTALLED. COUNTIES WILL BE REQUIRED TO MAINTAIN CONSTANT SEALS ON DEVICE AND WILL REQUIRE ADDITIONAL SEALS FOR PROTECTION AGAINST ENTRY POINTS AS INDICATED BY THE SECRETARY OF STATE. REFER TO GLOBAL CONDITION #5A FOR ENSURING INTEGRITY OF TRUSTED BUILD.

2) CROSS COMPATIBILITY

THE TESTING BOARD HAS DETERMINED THAT THE CARD ACTIVATOR IS COMPATIBLE FOR USE WITH EITHER THE EDGE2 OR EDGE2PLUS DRES

HAAT Model 50 Conditions (Version 2.1.18):

1) Intrusion Seals for Protection of Trusted Build Firmware.

Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on device and will require additional seals for protection against entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

2) CROSS COMPATIBILITY

THE TESTING BOARD HAS DETERMINED THAT THE HAAT IS COMPATIBLE FOR USE WITH EITHER THE EDGE2 OR EDGE2PLUS DRES.

